LEARNING MADE EASY

AWS Data Backup Essentials

Data doesn't protect itself. And despite providing what might well be the most secure and reliable compute platform the universe has ever seen, Amazon Web Services (AWS) can't guarantee that you'll never lose data, either. Here's a quick guide to understanding the threats facing your cloud data and mapping out a plan to protect yourself.

Threats Facing Cloud Data

Cloud Infrastructure Fails

Your Configurations Fail

Your Local Infrastructure Fails

Stuff Gets Destroyed by Accident — or Maliciously

You Can't Get Your Backup Up

Data that Deserves Protection is Missed or Overlooked

Love Your Data

The magic of AWS service and network integration makes it possible to greatly reduce the chances your application will go down. But your design must take the cloud's unique architectural features into account. Follow these best practices to make high availability an achievable goal.

Use Multiple Availability Zones

Replicate your compute instances and other resources across multiple Availability Zones. Even if one Availability Zone suffers an outage, your application remains accessible through the resources you launched in other zones.

Design Loosely Coupled Applications

Thinking about storing dynamic application data on your Amazon EC2 instances or within an AWS Lambda execution? The better solution is an application that writes its data to a highly resilient and stable platform — like an Amazon S3 bucket. An instance launched to replace one that just failed can simply query the Amazon S3 bucket to retrieve all the data it needs to complete its task.

Have a Cloud Data Protection Plan

Thinking about everything that might go wrong can turn into depression. But don't despair! With some moderate planning and preparation, you can build yourself a robust, wall-to-wall backup and recovery solution that's the next best thing to bulletproof.

1 Understand what your organization's operations demand.

How long can an outage last and how damaging can it be before it becomes impossible to get the business back on its feet again? Use these metrics:

Recovery Time Objective (RTO)

What's the maximum application downtime your organization can endure before you must be up and running again . . . or else?

Recovery Point Objective (RPO)

How much transaction and operational data (or how many customer transactions) can you afford to lose during an outage and still bounce back?

2 Consider the options for developing a data protection strategy.

Choose an option that meets your desired RTOs and RPOs, as well as the length of retention desired or required:

Amazon EBS snapshots

Because Amazon EBS volumes host your instance's operating system — along with any application data you maintain locally — it's the first thing you should target for backup.

Amazon S3

Consider how copying snapshots to more cost-effective Amazon S3 object storage tiers enables you to achieve long-term retention while saving on storage costs.

TIP

As powerful and flexible as those tools are, there's little chance they'll get you close to where you need to be to meet your RTO and RPO. For all but the simplest cloud deployments, you need a significantly more robust backup solution — something that covers your entire cloud, hybrid, and on-premises resource stack and offers a higher level of control and automation.

3 Optimize your backup operations.

From time to time during the process, step back and take a big-picture view. Your goal is optimization. Consider these strategies:

Address Risk

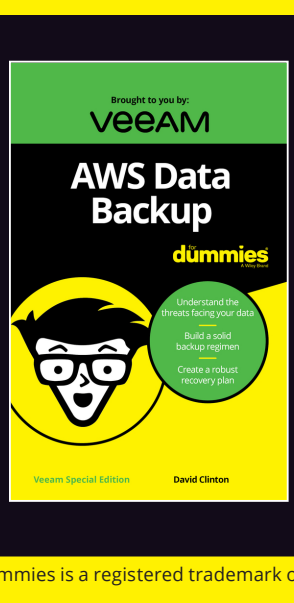
Isolate the resources used by your development, staging, and production layers into separate AWS accounts. Even if one account is brought down, you'll have the resources maintained within the others from which to rebuild. A well-designed third-party backup solution can smoothly orchestrate the whole process from a single control panel.

Control Backup Costs

Save money by carefully managing the storage lifecycles your backups will use. Data that you might need to access in a hurry should be kept as Amazon EBS snapshots. Older data that, perhaps, has to be kept available in case you're audited, could be stored in the much less expensive Amazon S3.

TIP

Backup cost estimation tools like those found in Veeam Backup for AWS help you proactively understand the financial impact of your backup policies before they surprise you when that monthly bill comes in.



To download your copy of *AWS Data Backup For Dummies*, go to https://go.veeam.com/wp-aws-backup-for-dummies

VEEAM

for dummies
A Wiley Brand

Wiley part no.: 978-1-119-82385-8